Natural Disasters in Cybersecurity

Bernard Ayuyao

Old Dominion University

CYSE 600 36666 Cybersecurity Principles

August 5, 2021

Natural Disasters in Cybersecurity

When you hear the word cybersecurity, what does that mean to you? What is your definition of cybersecurity? What do you think cybersecurity involves? For some, cybersecurity can mean defending their computer or portable and handheld electronic devices from hackers who are trying to attack them or their assets, business, or organization. Some may also say that it is a practice of protecting networks, systems, and programs from digital attacks. All this are true, but we are already overlooking at other things that can cause harm to our valued assets or systems which are natural disasters. There are many vulnerabilities that can make our valued assets useless, and a vulnerability is a type of weakness which can be exploited causing harm. When we think of threats, they can be a set of circumstances that has a potential to cause harm. Because when we think of cybersecurity, we think of threats from hackers trying to attack our computers, networks, systems, and programs. We must think outside of that box and look at what is already in front of our face and surroundings. Threats like natural disasters from flooding, fire, power loss, increase in surge of electricity and many more should be accounted for when thinking of potential threats to our most valued assets. To avoid threats from natural disasters, we must have a disaster recover plan. There are four distinct phases that encompasses this plan, and they are prevention and preparation, prerecovery, immediate recovery, and return-to-normal-operations.

The first step to disaster recovery planning is prevention and preparation. “During the prevention and preparation stage an assessment is made of the working environment and actions are implemented to avoid disaster or lessen its impact. Writers on the topic of disaster recovery planning state the first step is to determine which processes are critical.” (Rhode & Haskett, 1990, p. 853) This shows that when we plan we have to identify what we can do to avoid a threats from natural disaster. For example, when there is flooding, we can unplug any electrical outlets that can be exposed closely to water, raiser our personal computers and assets to a higher level, and put sand bags to prevent and eliminate as much water to come into the area we want protected from the flood. Only we know the operational environment that we are operating in so assessing it would help us create a plan to prevent the natural disaster that can effectively destroy our valued assets or systems.

Identifying preventative controls helps reduce risk or damage. “The team should figure out all the safe guards that have already been implemented by the organization to reduce redundancy. Furthermore, these controls should be measured to ensure that they can actually reduce the effects caused by business and system disruptions.” (Vuong, 2015) In the military, we have a process called operation risk management. It is a planning tool that helps the commander make a decision to continue with the mission because it shows all the risks involved. There are controls that are applied to every risk to reduce the risk that can cause harm to a person or crew. The same goes for identifying preventative controls because it allows the organization to determine what controls are needed to be put in place to continue operating that business if a disaster were to occur.

Planning allows a business or organization to recover. “Disaster recovery planning is the preparation for and recovery from a disaster. A proper DRP that has been enacted will enable the organization to restore operations back to normal after a disaster has struck the organization.” (Vuong, 2015) This shows that planning sets up an organization for success for both a plan and recovering from a disaster. A successful plan is when the plan is carried out what it is intended to do. For example, if a flood occurs due to a heavy storm and your plan was to put sandbags around the perimeter of the building to prevent water from coming in, and the end result of the plan was that your equipment was dry, then you had a successful plan. Also, planning allows for a successful recovery. For example, if you lose power or electricity from a storm, you can plan to have a back up generator that will provide electricity to the building. This allows the organization or business to recover from a power loss and continue to execute their mission from where they left off.

If a disaster occurs, we must also have a back up plan. “A key element in the prevention phase is data protection. Almost all groups have some items that must be stored off-site and some that must be fireproofed in house.” (Rhode & Haskett, 1990, p. 853) This shows that it would be smart to have a back up site because it allows a business to continue their operations when the other site goes down. It would also be smart to make this back up site located somewhere further from the original site because if they were together, they would both go down. A business should not put their eggs in one basket. All it takes is one strong hurricane to wipe out one whole area and everything in its path will be destroyed.

In case the key players or personnel are not available when disaster occurs, a laid out plan or document should be available. “The disaster recovery process is the development of the plan document. It “should contain detailed guidance and procedures for restoring a damaged system.” (Vuong, 2015) This is important because if the important personnel cannot be reached or available during the time of the disaster, it gives a step by step guidance on what to do to restore the system or keep the building and assets safe.

Fire is another natural disaster that we should be concerned about. “The business office has special needs for data protection. While much of its information is contained on floppy disks, there is an abundance of important material (e.g., personnel records and performance reviews), that is kept only in paper copy. A separate fireproof safe is required to ensure the privacy of many of these records." (Rhode & Haskett, 1990, p. 853) This shows that we have a lot of assets that we value. We need to plan ahead and store these items or assets into something safe and that something is a fireproof safe. If the building burns down, at least all the important documents, videos, files, copies, personal records, and many more, can be retained without any damage or it being destroyed.

This first step in a recovery plan is very important. "Prevention and preparation are the crux of disaster recovery. The care and thoroughness with which this phase is implemented will Determine how effectively recovery can be carried out in the event of an emergency." (Rhode & Haskett, 1990, p. 853) Without any preparation or planning, you plan to fail. Planning is important because it allows you to reach your intended goals and ensures you reach that goal whatever it may take. That back up plan is something you can rely on if your initial plan fails allowing you to continue with your mission.

With planning, there are two important facts that always and must be considered and they are required knowledge and required needs. Required knowledge is "the expected knowledge of potential issues, environment orientation and implementation, allocation of resources, and the determinacy of roles. The expected knowledge of potential issues relate to any and all adverse events that may happen to the organization as a whole or just in subsections of the organization. The impact of adverse events are unpredictable so having prior knowledge to certain likely scenarios will help mitigate some damages." (Vuong, 2015) This shows that knowing your threat gives you a good advantage because it allows you to plan for the worst. For example, it is like knowing your enemy's weakness. If you know their weakness then you can plan an attack, and the enemy can also prepare by making that weakness a lot stronger to prevent that attack. "To implement a proper plan, the adequate amount of investment must be made. The resources that need to be invested are not just money; it also includes time, people, software, and hardware. Money can buy the people, hardware, and software resources; however, experience at properly utilizing all the resources are a different story.” (Vuong, 2015) This also shows that an investment is needed to take care of your property and people because your property and equipment can be replaced but the skills and knowledge your people have may not be replaceable. It is important to plan for an investment like an insurance plan or training plan to apply those skills and knowledge to new employees that will help run your organization.

Required needs must also be considered when planning. “The second fact to consider is the task of creating a plan according to individual needs of the organization or company, including setting of all key parameters.” (Vuong, 2015) The entire organization must accept the disaster recovery plan because the plan will include or incorporate help of employees when it is adapted for use after a disaster has occurred. The plan that has been built but not carefully reviewed will end up with errors that are costly. This is like prioritizing your needs over wants. For example, if your organization is hit by a snow storm that is not threatening, it would be smart to shovel the pavement or apply salt to melt the snow rather than buying a snow plow. It would be nice to have a snow plow but it would be more of a want than a need. If the storm was strong enough, then that snow plow would turn into a need.

Business impact analysis is important because it helps the organization determine what is important and assigns priorities. “The business impact analysis was prepared to help identify and prioritize critical information and its host systems. Reviewing the business impact analysis allows the disaster recovery team to save time by not having to waste any resources on figuring out what is critical and important to the organization. The team can quickly acquire the needed information and go back to creating the disaster recovery plan.” (Vuong, 2015) Determining the cause and effect is important because it allows you to analyze what the impact is to your business or organization. When a tornado runs through town and its pathway is going through your business or organization, you can expect your building or facility to be destroyed and the tornado carrying assets like your computers and other physical assets with it. The impact is to determine the damage it caused to repair the building and what assets you have lost. After analyzing the impact, you can have a plan to recover from what was destroyed or lost. The computers may also have important data, so analyzing what data you have lost is important as well as having to prioritize what to backup before the disaster even happens.

Next, the second step to disaster recovery planning is prerecovery. “While preventative measures have been addressed in the previous phase, prerecovery encompasses those tasks, arrangements, or contacts which must be made in advance to ensure that effective recovery can begin in the event of a disaster. In this stage each staff member will assess what can be done to make recovery possible or easier.” (Rhode & Haskett, 1990, p. 853) This shows that if we do get hit by a disaster and it affects or disrupts our activities or prevents us from completing our mission, we can figure out how to recover from that issue. There must be a team or leader that will determine what are the next steps to recover from a disaster. For example, if we get hurt or cut by a knife, we put a band aid to recover from that cut. If the cut is deep enough, a doctor can determine what to do next and put stitches. The same goes for our valued assets like our computers and networks. Someone determines what should be done to continue the mission to keep the business running.

When recovering, there should be a person to be in charge. “During the prerecovery stage decisions should be made about who will be in charge and what roles people will play in the event of a disaster. This is the time for each staff member to take an inventory of his or her skills to determine whether he or she might be more useful in another area during an emergency." (Rhode & Haskett, 1990, pp. 853-854) There should only one person making the decisions and in charge. If there are many people in charge and making decisions, it would cause chaos and nothing will be done. Imagine having a room full of leaders, everyone would be arguing because they want to execute the plan their own way. When someone is in charge and everyone has their role and are executing in accordance with their role, recovery will flow a lot smoother. "The goal of prerecovery is for each person to know what he or she is to do in the event of a disaster." (Rhode & Haskett, 1990, p. 854) Everyone will know who will be called for assessing the damage, who will be contacted or determine an alternate computer location, and many more depending on what was planned by the person who is in charge.

A relocation is a good idea for the prerecovery phase. "The prerecovery phase encompasses most of the disaster recovery coordinator's work: making provisions for where the computing will be done and where the staff can be relocated in case of an emergency." (Rhode & Haskett, 1990, p. 854) In the Navy, we have what is called a COOP, or continuity of operations planning. It allows us to continue mission-essential functions in case a site goes down. The same goes for relocation. There can be hot or cold sites that can be activated when called upon. A cold site is a facility that is empty with no one working in it, also can be called a shell. When called upon to be activated, it can be manned, and equipment can be delivered in order to continue business operations that are essential. "A hot site may be more appropriate than a cold site. "A hot site is a computer facility with an installed and ready-to-run computing system. The system has peripherals, telecommunications lines, power supply, and even personnel ready to operate on short notice." (Pfleeger, Pfleeger, & Margulies, 2021, p. 698) I like to think of a hot site that is a cold site that is ready because you don’t need to provide equipment and power to operate, it is ready when called upon for operation.

Not all disasters are in the cyber realm and physical property must be considered. “The DRPs must also include considerations for the physical property of the organization. Information is an important piece to the core of the organization, but the physical property is the home for the information to reside and be used in. Failure to keep the physical assets secured or backed up will slowly, but surely, ruin the organization.” (Vuong, 2015) This shows that we must think outside of the cyber realm and think of what physical threats can happen. For example, if an earthquake happens, it can shake the whole building or facility which houses many computers and other important assets that provide service. If these are shaken and fall off, it can be destroyed and will be no longer of good use. A good solution to this problem is to secure the computer or assets by tying them down to prevent them from shifting or falling of a table or shelf. It would also be wise to keep your assets stored safely where it has a potential to fall and break.

The third distinct phase for a recovery plan is immediate recovery. “Immediate recovery includes those actions which must be taken to restore immediate computing capability and work environment. The activities of this phase are very dependent upon the nature and extent of the emergency situation. The initial task, however, is to assess the extent of the disaster and decide how much of the plan will be implemented.” (Rhode & Haskett, 1990, p. 855) This is just like when you fall and make a mistake, you must get up and recover from failure. In order to recover from failure, you must learn from your mistakes, that way you can plan your way ahead and apply those lessons learned to become successful and reach your goals, and in this case, ensuring your business is operating as intended to be.

Everyone in this phase must understand their role. “It is crucial for this phase that notification procedures (which had been determined in the prerecovery phase) operate flawlessly and that staff know what is expected of them. Tasks that might be necessary in this phase include damage assessment, sending damaged media to be salvaged, notifying alternate compute sites of the disaster and preparing to run critical operations at the emergency location.” (Rhode & Haskett, 1990, p. 855) This shows that if people understand their roles, the recovery procedure or phase can run much more smoothly. There would be no panic, false sense of emergency. Everyone understands what they need to do when disaster happens. It would also be beneficial if the staff have rehearsed or practice what they need to do in case of an emergency or disaster. They say practice makes perfect. We train like we fight and we fight like we train. Keeping us knowledgeable helps us not lose focus and more rehearsed or aware in an event happens because it becomes like muscle memory.

What also comes with training is testing. “Test the plan with the use of employee training and exercises. These tests help by finding the errors or failures that occur and fixing them, ultimately improving the plan.” (Vuong, 2015) This shows that testing is important because it allows you to catch what went wrong instead of figuring and finding out everything that the plan was not actually a good plan when disaster happens. This testing and training also keeps everyone ready and proficient on what to do. Also, things change and maintaining this disaster recovery plan is important. The plan should be reviewed and updated regularly because new ideas may be thought of, you can incorporate new methods, technology, or personnel into the new and improved plan.

The internet is a great tool for recovering. “For many of us, the Internet has become an important, if not critical, part of daily life. After a disaster, it can be the best (if not the only) way to get early messages to family and friends. But our dependence on the Internet carries its own risks, and we should prepare for those as well. Although it's not as crucial as food or water, information can play an important part in recovering from a disaster. The more accessible that information is to you when you really need it, the easier your recovery will be." (Treese, p. 17) This shows us that the internet is helpful when disaster strikes because it can be a tool for accessing information. Phone lines can get tied up when trying to reach your family. Luckily, we can rely on the internet when you need to get the latest news of what happened during the disaster. The news can be accessed immediately and social media or Facebook messenger can be a used to communicate when needed.

The internet can also be used for saving important information. "The Internet offers a wide set of choices for storing data remotely. Users of email services such as Yahoo!, Gmail, and Hotmail are already storing some information offsite, and their access to that email is not affected by a disaster at home." (Treese, p. 16) We can use our emails to store and send ourselves anything of importance in preparation for disaster. Any important data like photos, financial information that can be kept in our email. It is great to take advantage of this because it is a free service. Another option is to use cloud services. There are some free cloud services and some that you can pay for to upgrade the amount of storage your organization or company needs. CDs or DVDs are also an option for backing up and storing data. The only problem is that they can get lost or misplaced.

Information plays a big role when preparing for a disaster. "For many of us, the Internet has become an important, if not critical, part of daily life. After a disaster, it can be the best (if not the only) way to get early messages to family and friends. But our dependence on the Internet carries its own risks, and we should prepare for those as well. Although it’s not as crucial as food or water, information can play an important part in recovering from a disaster. The more accessible that information is to you when you really need it, the easier your recovery will be.” (Treese, p. 17) When we watch the news we gather information to help us make a sound decision. Watching the weatherman giving details about the daily forecast is information that can be used on where to go if a hurricane passes by, how long the storm will last will help us gather the right amount of food and supplies during the timeframe, and details about flooding and wind gusts to help us prepare our homes to withstand possible damage that may occur. Without information, we can get blindsided from a natural disaster that can be costly from both money or someone’s life.

Once gathering all the information you need, it must be prioritized when planning. “Making those choices can get complicated because the amount of information each of us stores is constantly increasing. Much of it isn’t crucial, but sorting it out can seem like more trouble than it’s worth. If you are trying to keep track of the most important data, key items to remember are photos and financial information. Surveys indicate that one of the main items people would choose to rescue from a burning house are family photos, so don’t forget the digital pictures. The same goes for video, though the required disk space may be daunting. Save copies on DVD offsite instead.” (Treese, p. 16) This shows that we can’t save every single thing we own when a disaster occurs. Family photos are important because those are memories that can’t be brought back in person when you lose them but you must also keep in mind that family photos are not going to help you survive a hurricane. Food, gas, shelter, electricity, and other essential items are what is needed to survive because those are items that will help you continue living throughout the day.

Keeping important data virtualized can be helpful when dealing with disasters. "Virtualization would be the use of the cloud computing software to store information on the Internet. The backup thought is the method of storing information at different locations using different storage methods such as USB drives, external hard drives, or actual paper files. Virtualization can be considered a type of backup method as well." (Vuong, 2015) Sometimes keeping your most important data virtualized can save it from physical damage, in this case a natural disaster like a hurricane, tornado, or earthquake. Actual papers can be torn, burned, or damaged from a flood which will not be helpful when trying to recover. Saving those files virtually can be recovered easily.

The final step of the distinct phase of this recovery plan is to retorn-to-normal operations. "Return-to-normal operations includes all those steps necessary to restore computing capabilities and work environment to their predisaster state. This includes activities such as the purchase of new computers, restoration of facilities, and return of users to original computing environment." (Rhode & Haskett, 1990, p. 855) This shows that when a disaster hits, we must continue operating like we usually do. To continue off where the business or company left off, the business may need to purchase new equipment because of the equipment that got destroyed from the disaster. This can cost money but can favor changes in the company because old and outdated equipment can be replaced by new and better ones.

All in all, when we look at cybersecurity, we think of someone trying to hack our computers or put a malicious code into our systems. The picture that we usually imagine about cybersecurity focuses on the integrity and confidentiality of our systems. We tend to forget that cybersecurity also deals with our physical assets that can be vulnerable to natural disasters which affects the availability of our assets. No one knows exactly when disaster can happen but we can always be prepared for when it strikes. In order to be prepared we have four phases of planning which are prevention and preparation, prerecovery, immediate recovery, and return-to-normal-operations. If we follow these four distinct phases of our plan, we can lessen the damage of what a natural disaster may have done to our systems or most valuable assets and data.

References

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2021). Problems with Use of Biometrics. In *Security in Computing Fifth Edition* (p. 55). Uttar Pradesh: Pearson Education, Inc.

Rhode, R., & Haskett, J. (1990, June). Disaster Recovery Planning For Academic Computing Centers. *33*(6). Retrieved from https://dl-acm-org.proxy.lib.odu.edu/doi/pdf/10.1145/78973.78975

Treese, W. (n.d.). PLANNING FOR DISASTER WITH THE INTERNET. Retrieved from https://dl-acm-org.proxy.lib.odu.edu/doi/pdf/10.1145/1103940.1103952

Vuong, J. (2015, October). Disaster Recovery Planning. Retrieved from https://dl-acm-org.proxy.lib.odu.edu/doi/pdf/10.1145/2885990.2886006